In the claims:

Kindly amend the claims to read as follows:

1. (Amended) A system for supporting mutually exclusive program execution, the system [A system that is operable to insure authorized access to secured repositories of data and programs, to support protected mutually exclusive execution of programs,] comprising:

a first component operable to provide authorized access to secured repositories of data and programs, to prevent one application from utilizing, scrutinizing or modifying another application,

a second component operable to execute programs loaded from or residing in said repositories of programs and accessing said repositories of data,

said first and second components operating in parallel,

wherein the first component comprises a SAM; and

wherein the second component comprises a computing application environment, separated from the SAM by SAM-access controlling rules, and operable to execute operations, use of which is regulated by the SAM, on at least one of the following: downloaded data downloaded from said repositories by said SAM; and firewall-protected random access data;

wherein the use of the downloaded data by the computing application environment, and access of the computing application environment to the downloaded data, are regulated by the SAM;

and wherein the firewall-protected random access data is stored in memory which is made accessible to said computing application environment only by the SAM.

2. (Original) The system of claim 1, containing a coordination medium, said coordination medium being operable to conveying information between a plurality of sub-modules within said system, and being operated in compliance with a security rule whereby said coordination medium is detached from the control of any program loaded from or residing in said repositories of programs whenever said coordination medium is attached to said data repositories.

3. (Original) The system of claim 1, wherein said repositories of programs are operable to fetch for execution portions of a complete program during program run time.

4. (Amended) The system of [According to] claim 3, wherein fetching of portions of a program are subject to a mask controlled by said first component, said mask being a plurality of control values determining which parts of said repositories of programs are operable in an application session.

5. (Cancelled)

6. (Original) The system of claim 1, operable in a mobile communication device.

7. (Original) The system of claim 1, implemented on a single monolithic microelectronic circuit.

8. (Amended) The system of claim 1, wherein traffic of information between parts of the system that do not reside on a common monolithic microelectronic integrated circuit is typically encrypted.

9. (Amended) The system of claim 1, [containing an] also comprising apparatus for personal identification.

10. (Amended) The method of claim [5] 49 wherein said [controlling of] access to [secured] repositories [of data and programs] is controlled based on public key encryption.

11. (Amended) The method of claim [5] 49 wherein said authorized access [downloading of executable programs] is based on public key encryption.

12. (Amended) A method according to claim [5] 49, wherein applications are exclusively authorized by a certified authority identifiable to the [TCE] SAM, whereby such authority's public key is

immutably programmed into [the TCE SAM's] a non-volatile memory in the SAM, wherein confidential client programs are licensed to be programmed into, updated and improved after verifiable certification of said authority.

13. (Amended) A method according to claim [5] 49 wherein a plurality of authorities are licensed to program applications into [the TCE SAM's] a non-volatile memory [in the SAM].

14. (Amended) A [method] system according to claim 1, wherein at least one analog input to the application environment is operative to input analog data.

15. (Amended) A method according to claim [5], 49 wherein at least one analog input to the application environment is operative to input analog data.

16. (Amended) A [method] system according to claim 14 wherein said input data corresponds to an image.

17. (Original) A method according to claim 15 wherein said input data corresponds to an image.

18. (Amended) A [method] system according to claim 16 [1,] wherein said image is derived from the output of a fingerprint detector operative to provide data for feature extraction [typically to prepare a feature matrix to identify the possessor of said fingerprint].

19. (Amended) A method according to claim [5,] 17, wherein said image is derived from the output of a fingerprint detector operative to provide data for feature extraction [typically to prepare a feature matrix to identify the possessor of said fingerprint].

20. (Amended) A [method] system according to claim 1, wherein the fingerprint detector is operative to prepare a feature template to identify the possessor of said fingerprint and wherein said sensed feature [matrix] template is compared to at least one [trained matrix] stored

feature template residing in the secured [memory repository.] repositories

21. (Amended) A method according to claim [5,] 49 wherein the fingerprint detector is operative to prepare a feature template to identify the possessor of said fingerprint and wherein said sensed feature [matrix] template is compared to at least one [trained matrix] stored feature template residing in the secured [memory repository.] repositories

22. (Amended) A [method] system according to claim [1,] 14wherein the analog data corresponds to a voice message.

23. (Amended) A method according to claim[5,] 15 wherein the analog data corresponds to a voice message.

24. (Amended) A [method] system according to claim 22, wherein features are extracted from the voice message [operable] in order to identify a [the] speaker of the voice message.

25. (Amended) A method according to claim 23, wherein features are extracted from the voice message [operable] in order to identify a [the] speaker of the voice message.

26. (Amended) A [method] system according to claim 1, wherein previous to initializing an application session no application data pertaining to a previous application session remains in the application environment [partition].

27. (Amended) A method according to claim [5,] 49 wherein previous to initializing an application session no application data pertaining to a previous application session remains in the application environment [partition].

28. (Amended) A [method] system according to claim 1, wherein said repositories of data and programs comprises executable memory and data memory and wherein following an application session, said executable memory and data memory are [all] reset.

29. (Amended) A method according to claim [5,] 49 wherein said repositories of data and programs comprises executable memory and data memory and wherein following an application session, said executable memory and data memory are [all] reset.

30. (Amended) A [method] system according to claim 1, wherein [the circuits] at least a portion of the first and second components are embedded in smart cards.

31. (Amended) A method according to claim[s 5,] 49 wherein [the circuits] at least a portion of the first and second components are embedded in smart cards.

32. (Amended) A [method] system according to claim 1 wherein at least a portion of the first and second components [the circuits] are embedded in [the] subscriber identification modules of mobile communication devices.

33. (Amended) A method according to claim [5] 49 wherein at least a portion of the first and second components [the circuits] are embedded in [the] subscriber identification modules of mobile communication devices.

34. (Amended) A [method] system according to claim 1 wherein at least a portion of the first and second components [the circuits] are operable to enhance security and functionality in computer network servers.

35. (Amended) A method according to claim [5] 49 wherein at least a portion of the first and second components [the circuits] are operable to enhance security and functionality in computer network servers.

36. (Amended) A [method] system according to claim 1 wherein at least a portion of the first and second components [the circuits] are operable to enhance security and functionality of mass storage devices.

37. (Amended) A method according to claim [5] 49 wherein at least a

portion of the first and second components [the circuits] are operable to enhance security and functionality of mass storage devices.

38. (Amended) A [method] system according to claim[s] 1 wherein at least a portion of the first and second components [the circuits] are operable to enhance security and functionality of computing devices.

39. (Amended) A [method] system according to claim[s] 1 wherein at least a portion of the first and second components [the circuits] are operable to enhance security and functionality of computing devices.

40. (Amended) A [method] system according to claim 1 wherein the system [can] is operative to authenticate the validity and integrity of multi-origin data files.

41. (Amended) A method according to claim [5] 49 [wherein the system can authenticate] and also comprising authenticating the validity and integrity of multi-origin data files.

42. (Amended) A [method] system according to claim 14, wherein visual data[,] is input in clear text to the application computing environment and is synchronized with audio data which is decompressed by [in] the [device] system wherein both [media] visual and audio data are output simultaneously in separate streams to a [the] display device.

43. (Amended) A method according to claim 15, wherein visual data[,] is input in clear text to the application computing environment and is synchronized with audio data which is decompressed [in the device] wherein both [media] visual and audio data are output simultaneously in separate streams to a [the] display device.

44. (Amended) A [method] system according to claim 16, wherein fine tuning portions of visual data residing in the data repository are intertwined with [the] audio data [of] in the SAM and are typically operative to enhance [the] visual data input in the clear from a [the] host, to thereby typically prevent quality duplication of the [digitized] visual

data.

45. (Amended) A method according to claim 17, wherein fine tuning portions of visual data residing in the data repository are intertwined with [the] audio data [of] in the SAM and are typically operative to enhance [the] visual data input in the clear from a [the] host, to thereby typically prevent quality duplication of the [digitized] visual data.

46. (Original) The system of claim 1, embedded within a wireless communication device.

47. (Original) The system of claim 1, serving a credit or debit charge card clearance scheme.

48. (Original) The system of claim 1, operative to display flight schedule, to reserve flights, to ticket flights, and to clear payments for airline services.

49. (New) A method for supporting mutually exclusive program execution, the method comprising:

providing a first component operable to provide authorized access to secured repositories of data and programs, to prevent one application from utilizing, scrutinizing or modifying another application; and

providing a second component operable to execute programs loaded from or residing in said repositories of programs and accessing said repositories of data,

said first and second components operating in parallel,

wherein the first component comprises a SAM; and

wherein the second component comprises a computing application environment, separated from the SAM by SAM-access controlling rules, and operable to execute operations, use of which is regulated by the SAM, on at least one of the following: downloaded data downloaded from said repositories by said SAM; and firewall-protected random access data;

wherein the use of the downloaded data by the computing

application environment, and access of the computing application environment to the downloaded data, are regulated by the SAM;

and wherein the firewall-protected random access data is stored in memory which is made accessible to said computing application environment only by the SAM.